Peer Reviewed Refered
and UGC Listed Journal
Journal No.: 47100

AN INTERNATIONAL MULTIDISCIPLINARY
HALF YEARLY RESEARCH JOURNAL

GENIUS

Volume - VI, Issue - II, FEBRUARY - JULY - 2018
ISSN - 2279 - 0489

Impact Factor - 4.954 (www.sjifactor.com)

PART - III

AJANTA PRAKASHAN

Kautika H Churi

ISSN 2279 - 0489

AN INTERNATIONAL MULTIDISCIPLINARY
HALF YEARLY RESEARCH JOURNAL

GENIUS

Volume - VI | Issue - II | PART - III | February - July - 2018

Peer Reviewed Referred and UGC Listed Journal

Journal No. 47100

ज्ञान-विज्ञान विमुक्तये

IMPACT FACTOR / INDEXING
2017 - 4.954
www.sjifactor.com

❖ EDITOR ❖

Assit. Prof. Vinay Shankarrao Hatole
M.Sc (Math's), M.B.A. (Mkt), M.B.A (H.R),
M.Drama (Acting), M.Drama (Prod & Dirt), M.Ed.

❖ PUBLISHED BY ❖

Ajanta Prakashan
Aurangabad. (M.S.)

CONTENTS OF PART - III

CONTENTS OF PART - III

Volume - VI - Issue - II - February - July - 2018
GENIUS - ISSN - 2279 - 0489 - IMPACT FACTOR - 4.954 (www.sjifactor.com)

CONTENTS OF COMMERCE

8

Keyloggers: Monitoring and Security Web Activity in Workplace

Juita Tushar Raut
Assistant Professor, Departmentof IT Sonopant Dandekar College, Palghar.
Sayli Mandar Bhosale
Assistant Professor, Departmentof IT Sonopant Dandekar College, Palghar.

Abstract

A keylogger is software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you don't know that your actions are being monitored.

In this paper we provide an explanation of keyloggers, the different types and the history. These tools can be used for good causes like monitoring the web activity of employees in workplace. This technology is both a blessing and a curse in the employment arena. Sophisticated monitoring software and hardware allow businesses to conduct basic business transactions, avoid liability, conduct investigations and ultimately, achieve success in a competitive global environment. Employees can also benefit when monitoring provides immediate feedback, keeps the workforce efficient and focused and discourages unethical/illegal behavior.

Keywords: Keyloggers, unethical, illegal, liability, investigation etc.

Introduction

Keyloggers have somewhat of a bad reputation in the technology world because more often it's associated with illegal spying and theft of personal and monetary information. In reality even though that's one of the main uses, it can be used for other more appropriate and legal tasks. One clear example of this would be at a company's security. By logging his activity on his workstation the company may be able to confirm their suspicions or clear his name. Sometimes a simple and inexpensive tool like Keyloggers may save companies millions in damages.

Keyloggers are fall into four main categories: Software-based Keyloggers, Hardware-based Keyloggers, Acoustic Keylogger and Wireless Keyloggers.They have different implications and different information capturing process.

Software-based Keyloggers- Software Keyloggers track systems, co data within the target operating system, store them on disk or in remote loca them to the attacker who installed the Keyloggers. The main advantag Keyloggers compared to the hardware Keyloggers is that they can run for amount of time while the info is being transmitted remotely eliminating personally obtain the information like it's the case with hardware Keyloggers.

Hardware-based Keyloggers – Hardware Keyloggers are small elec used for capturing the data in between the computer and the personal comp capable to trap nearly anything instead all kinds of things whatever you ty computer keyboard. Several lately composed keyloggers have the ability to a pictures of the computer's desktop and many duplicate every little thing that is hardware keylogger has an advantage over a software solution: it is not depen installed on the target computer's operating system and therefore will not inter program running on the target machine or be detected by any software.

Acoustic keylogger- Acoustic keylogger can be used to monitor the sou someone typing on a computer. Each key on the keyboard makes a subtly dif signature when struck. It is then possible to identify which keystroke signa which keyboard character via statistical methods such as frequency analysis.

Wireless keylogger - Wireless Keylogger consists of two main buildi transmitter, and the receiver. The actual keylogging takes place in the transmit fact a PS/2 hardware keylogger, with a built-in 2.4 GHz wireless module. Capt data is transmitted through the radio-link in real-time, rather than getting stored on the other hand, is a wireless acquisition unit with a USB interface. All received from the transmitter is sent to the host computer via USB.

History

Even though these devices are relatively new to us, Keyloggers hav with us almost half of a century. Their exact history cannot be known perfe believed that they first were used by the government and obviously they do n exact day.

It captures every key pressed on the keyboard and stores in a file, ma external device that can be viewed by

There are many reasons why you may need an internet history keylogger. The obvious reason is to investigate someone online activity and discover what ever information you may find valuable.

Although these products were once known as hacker tool, they are now used commonly on home and office computers. Companies use this software to monitor theiremployeesactivity to ensure company rules are followed and secrets are not being shared.

Security

Keyloggers can help employers maintain productivity, Boost Performance, Eliminate Corruption, protect valuable bandwidth and ensure optimum use of networked resources by monitoring employee activity online. Employees working hard lead to an increase in the overall performance of the company.

The latest breed of hardware Keyloggers are much harder to detect since they do not install any code onto the machine and cannot be spotted by traditional anti-virus or anti-spyware tools. They are, therefore, becoming more common as determined criminals realize that the returns to be gained from software versions have diminished. Certainly in large organizations it isn't practical for the IT security manager to manually check the back of every single box and every single keyboard. Secondly, they should consider the type of equipment that is used in the organization.

Even though that both hardware and software Keyloggers are known, software Keyloggers are the ones that are being widely used due to the inexpensive and easier to implement onto a computer. Each different operating system will have an adapted Keyloggers which suits the I/O. Monitoring keystrokes will help with the work flow, investigation theft, review performance, prevent harassment, missing data and prevent personal use.

Work flow will increase due to the fact that the employees will be motivated, this will weed out the employees that want to go on Facebook or check their personal emails which might cause a security leak. If there is some type of deleted file or missing information the security personnel can detect which computer that is missing such important information and figure out what went wrong. Employees knowing all this will show performance at their job from the amount of keystrokes they had to do. If someone is being harassed then this will

increase the chances of finding out whom and when the incident occurred. In the end it prevent personal use and increase safety and security with other benefits.

Implementation

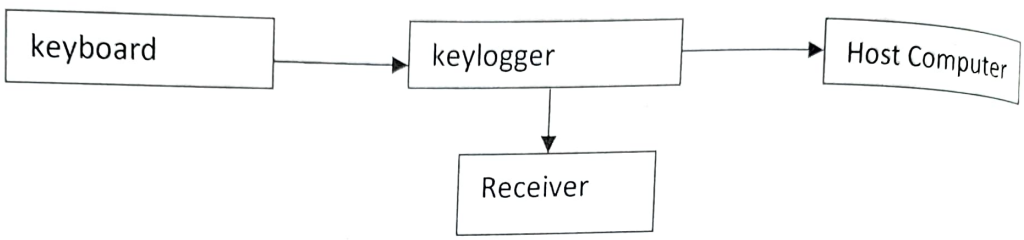
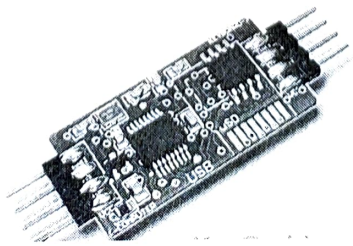


Fig. Block diagram of Keylooger system

The implementation of Keylogger and design are based upon many factors: the of operating system, the lifespan of a Keylogger, where it is infecting and the level footprint on a machine. There are two predominant types of hardware keyloggers. The first a keyboard adapter type that is installed inline by plugging the adapter into the keyboard then plugging the keyboard into the adapter. Installed in this manner, it can easily intercept the traffic between the keyboard and the workstation. Note that this variety of keylogger comes in both PS/2 and USB flavors.

The other type of hardware keylogger is the module type that is actually a very small PCB. This device is installed inside the keyboard where it can evade detection. Installation takes more time and effort, but it is stealthy and provides the same functionality as an external adapter type. With this keylogger, security awareness training is less helpful than with the visible adapter type.



Software Keyloggers are made to ensure proper installation by web browser exploit for example. Security vulnerabilities vary depending on the browser being used and the attacker can identify and exploit the weaknesses. An attack can be executed by utilizing JavaScript which could be a user side language.

The Wireless Keylogger consists of two main building blocks: the transmitter, and the receiver. The actual keylogging takes place in the transmitter, which is in fact a PS/2 hardware keylogger, with a built-in 2.4 GHz wireless module. Captured keystroke data is transmitted through the radio-link in real-time, rather than getting stored. The receiver on the other hand, is a wireless acquisition unit with a USB interface. All keystroke data received from the transmitter is sent to the host computer via USB. From the software side, this data is available through a virtual COM port, allowing any terminal client to be used for visualizing keystroke data.

Conclusion

We examined the current state of Keyloggers and how they can spread.Although Keyloggers have a bad reputation in society, the research done to elaborate this paper shows how these devices can be used not always in a malicious way of action such as illegal spying and theft of personal information. At a company level, Keyloggers can be used to monitor any suspicious activity that may cause a serious liability to the company`s benefit. Workers who are under doubt can be explicitly be discover or clear their names. This helps the company ensure their interests before any bigger security issue happens, making them save larger quantities of money. Another legal way of using a Keylogger is in a closer and more personal level, home.Nowadays, there are a lot of people looking for victims online. Child`s predator, kidnappers, and so all are always seeking innocent children, and Keyloggers can be very helpful in order to minimize those kinds of attacks from occurring.

References

1. https://www.keelog.com/wireless_keylogger.html
2. http://www.bcs.org/content/conWebDoc/11115
3. https://en.wikipedia.org/wiki/Hardware_keylogger
4. http://www.spybulletin.com/different-types-of-keyloggers/
5. www.google.com